



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/927,427	08/08/2001	Michael Howard	MS1-909US	6390
22801	7590	09/06/2006	EXAMINER	
LEE & HAYES PLLC 421 W RIVERSIDE AVENUE SUITE 500 SPOKANE, WA 99201			TESLOVICH, TAMARA	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 09/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/927,427

Applicant(s)

HOWARD ET AL.

Examiner

Tamara Teslovich

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 10 July 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-31 and 33-44 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-31 and 33-44 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 7/10/06.

- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

This Office Action is in response to the Remarks and Amendments filed on July 10, 2006.

Claims 1, 3-7, 11, 13-14, 16-17, 21, 23-24, 26-27, and 31 have been amended.

Claims 37-44 are new.

Claim 32 has been canceled.

Claims 1-31, and 33-44 are pending and herein considered.

### ***Response to Arguments***

Applicant's arguments concerning the Examiner's rejections of claims 1-10 as being directed to non-statutory subject matter are considered but not persuasive. In response to the Applicant's arguments concerning the Examiner's previously given 101 rejections to claims 1-10, the Examiner respectfully disagrees that the Applicant's amendments have overcome the rejections.

Additionally, claims 1-10 are now also rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention as a result of the newly added limitations, namely "providing the identified set of potential security threats." It is unclear to whom exactly the identified set of potential security threats is provided or by what means.

Applicant's arguments concerning the Examiner's previously given 102(a) rejection of claims 1-36 and the obviation of the Examiner's grounds for rejection based upon the amendments to independent claims 1, 11, 21, and 31 are considered but not persuasive. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Therefore, based on the above arguments, the Examiner maintains the 35 USC § 102 rejections of claims 1-36 as set forth in the previous office action and amended below in accordance with the Applicant's amendments. Additionally, newly added claims 37-44 are rejected below.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention based upon the newly added limitation of "providing the identified set of potential security threats" to claim 1. It is unclear from this to whom exactly the identified set of potential security threats is provided or by what means. Claims 2-10 depend upon rejected claim 1 and are rejected for the same reasons.

***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-10 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The language of claim 1 raises a question as to whether the claim is directed merely to a method that is not tied to a technological art, environment, or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

**Claims 1-36 are rejected under 35 U.S.C. 102(a) as being anticipated by “*Security Analysis & Design*” by Uttara Nerurkar, hereinafter referred to as Nerurkar.**

As per **claim 1**, Nerurkar discloses in a computer system, a method for providing application security threat-modeling, the method comprising providing class definitions

Art Unit: 2137

for a plurality of model (software and hardware) components (peels) to represent respective elements of an application (pg.50 col.3 par.4), each class definition specifying a set of potential security threats associated with the model components (security concerns) (pg.50 col.2 par.2); responsive to user input, interconnecting at least a subset of the model components to form a logical model ("onion diagram") of the application (pg.52 col.1 par.1); marking one of the potential security threats associated with a selected model component as a countered security threat (page 56 col.2 par.2); automatically analyzing the at least a subset of model components and respective interconnections to identify a set of potential security threats corresponding to the at least a subset, the potential security threats being associated with one or more of the security threat categories; and providing the identified set of potential security threats (pg.52 col.1 par.3; pg.54 col.1 par.3).

As per **claim 2**, Nerurkar discloses the method of claim 1, wherein the model components comprise a module, a port, a store, or a wire (network cabling) (pg.50 col.3 par.4).

As per **claim 3**, Nerurkar discloses the method of claim 1, wherein the potential security threats comprise at least one subset of authentication (IA), authorization (AZ), auditing (OO), privacy, integrity (OO), availability, and non-repudiation (pg.56 col.1 par.3)

As per **claim 4**, Nerurkar discloses the method of claim 1, wherein providing the class definitions further comprises determining the potential security threats based on

functionality of the component with respect to the application (use of objects in the zone) (pg.50 col.2 par.2).

As per **claim 5**, Nerurkar discloses the method of claim 1, wherein analyzing further comprises responsive to selection of a particular component of the model components displaying each other component of the at least a subset that comprise at least a subset of similar potential security threat categories as the particular component (partition based on the similarity and nature of security concerns of the components) (pg.52 col.1 par3).

As per **claim 6**, Nerurkar discloses the method of claim 1, further comprising marking an additional potential security threat associated with a second selected component as a second countered security threat, wherein the second countered security threat and the countered security threat are substantially the same security threat; and wherein analyzing further comprises responsive to selection of a the second selected component, automatically highlighting the selected component (page 56 col.2 par.2)

As per **claim 7**, Nerurkar discloses the method of claim 1, wherein analyzing further comprises providing for the selection of a particular threat to indicate that the particular threat requires a threat mitigating implementation in a particular model component of the at least a subset (pg.50 col.3 par.1; pg.56 col.2 par.2).

As per **claim 8**, Nerurkar discloses the method of claim 7, wherein providing for the selection of the particular threat further comprises identifying a priority of the threat

mitigating implementation (decompose into sets consisting of objects requiring similar levels of security) (pg.54 col.1 par.3).

As per **claim 9**, Nerurkar discloses the method of claim 7, wherein providing for the selection of the particular threat further comprises identifying a desired level of strength of (control) technology with which to mitigate the particular threat (pg.56 col.2 par.2).

As per **claim 10**, Neruarkar discloses the method of claim 7, wherein providing for selection of the particular threat further comprises presenting information associated with a particular technology (design and choose countermeasures based on coverage and costs) with which to mitigate the one or more potential threats in a physical implementation of the application (pg.50 col.3 par.1).

Claims **11-20** are directed towards a software implementation of the method of claims 1-10 and are rejected by a similar rationale.

Claims **21-30** are directed towards a computer system implementing the method of claims 1-10 and are rejected by a similar rationale.

Claims **31-33** are directed to a user interface comprising means for the implementation of the method of claims 1-3 and are rejected by a similar rationale.

Claims **34-36** are directed to a user interface comprising means for the implementation of the method of claims 8-10 and are rejected by a similar rationale.

As per **claim 37**, Neruarkar discloses the method of claim 1, further comprising determining that the countered security threat neutralized one of the potential security



threats associated with a model component other than the selected model component; and revising the set of potential security threats associated with at least one of model components other than the selected model component by removing the neutralized potential security threat from the set (page 56 col.2 par.2).

As per **claim 38**, Neruarkar discloses the method of claim 37, further comprising automatically generating computer code configured to prevent the potential security threat marked as the countered security threat in response to the marking (page 56 col.2 par.2).

As per **claim 39**, Neruarkar discloses the method of claim 11, further comprising instruction for determining that the countered security threat neutralized one of the potential security threats associated with a model component other than the selected model component; and revising the set of potential security threats associated with at least one model components other than the selected mode component by removing the neutralized potential security threat from the set (page 56 col.2 par.2).

As per **claim 40**, Neruarkar discloses the method of claim 39, further comprising instructions for automatically generating computer code configured to prevent the potential security threat marked as the countered security threat in response to the marking (page 56 col.2 par.2).

As per **claim 41**, Neruarkar discloses the method of claim 21, wherein the computer-executable instructions further comprise instructions for determining that the countered security threat neutralizes one of the potential security threats associated with a model component other than the selected model component; and revising the set

of potential security threats associated with at least one of model components other than the selected mode component by removing the neutralized potential security threat from the set (page 56 col.2 par.2).

As per **claim 42**, Neruarkar discloses the method of claim 41, wherein the computer-executable instructions further comprise instructions for automatically generating computer code configured to prevent the potential security threat marked as the countered security threat in response to the marking (page 56 col.2 par.2).

As per **claim 43**, Neruarkar discloses the method of claim 31, wherein the processing means further comprise means for determining that the countered security threat neutralizes one of the potential security threats associated with a model component other than the selected model component; and means for revising the set of potential security threats associated with at least one of model components other than the selected mode component by removing the neutralized potential security threat from the set (page 56 col.2 par.2).

As per **claim 44**, Neruarkar discloses the method of claim 43, wherein the processing means further comprises instructions for automatically generating computer code configured to prevent the potential security threat marked as the countered security threat in response to the marking (page 56 col.2 par.2).

### ***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

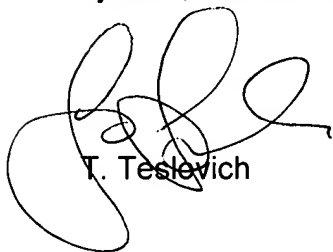
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



T. Teslevich



EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER